Firefox "Security" — The OpenSnitch Truth

What Firefox Told You

"We protect you with Safe Browsing — it checks URLs against known malicious sites to keep you safe."

What OpenSnitch Showed Us

Every connection Firefox made — silently, automatically, without asking — in the name of that "security."

The Connections Firefox Was Making to Google

Setting	What It Claims	What It Actually Does
`safebrowsing.malware.enabled`	Blocks malware sites	Sends URL data to Google servers every 30 min
`safebrowsing.provider.google5.enabled`	Hidden v5 provider	Contacts Google even after disabling the main toggle
`geo.provider.network.url`	Location services	Sends geolocation requests to googleapis.com
`dom.push.enabled`	Push notifications	Maintains persistent connection to Mozilla/Google infrastructure
`network.captive-portal-service.enabled`	Detects captive portals	Phones home on every network change
`network.connectivity-service.enabled`	Checks connectivity	Regular beaconing to external servers

---

The Architecture of the Deception

USER SEES:

```
"Safe Browsing: Protection against dangerous sites" ✅
```

OPENSNITCH SEES:

```
firefox-bin → safebrowsing.google.com  → POST URL data
firefox-bin → googleapis.com           → GET geolocation
firefox-bin → 142.251.x.x (Google)     → repeated connections
firefox-bin → 172.217.x.x (Google)     → repeated connections
```

Google receives:

- Your IP address (or VPN exit if using one)
- Timing patterns of your browsing
- URL fragments for "checking"
- Your approximate location
- Connection frequency building a behavioral profile

The google5 Smoking Gun

The most revealing discovery — Firefox has **three** separate Google Safe Browsing providers:

```
google   ← v2, older
google4  ← v4
google5  ← v5, newest, has its OWN enabled flag
```

When users disable Safe Browsing through the standard interface, they disable `google` and `google4`. `google5` **has a completely separate enabled toggle that remains** `true` — invisible to the standard settings UI, buried in `about:config`.

```
browser.safebrowsing.provider.google5.enabled = true
        ↓
Silently contacting:
safebrowsing.googleapis.com/v5/hashes:search
safebrowsing.googleapis.com/v5/hashLists:batchGet
```

This is not an accident. This is **architecture.**

The Principle at Work

Security Theater Formula:

> Visible setting that satisfies user concern
>
> - Hidden secondary mechanism that preserves data collection = User feels protected. Google gets data.

Mozilla's largest single revenue source is their Google search deal — $400M+/year. The incentive structure is not aligned with user privacy, regardless of public statements.

What Actually Protects You

What Firefox called "security":

- Google Safe Browsing — sends your data to Google

What actually protects you:

- **uBlock Origin** (medium mode) — blocks malicious domains *locally*
- **Mullvad DNS content blockers** — blocks at DNS level before connection

No data sent anywhere. No Google in the chain. The protection you have *without* Safe Browsing is technically superior to the protection Safe Browsing provides — because it operates locally, with no external surveillance component.

The OpenSnitch Principle

OpenSnitch doesn't care what an application says it does. It watches what it *actually* does at the network level — every connection attempt, every destination, every process.

```
Marketing copy  =  what they want you to believe
OpenSnitch log  =  what is actually happening
```

The gap between those two things is where surveillance lives.

> *"The most dangerous deception is the one wearing the face of your protection."*

That's not paranoia. That's what the logs showed.

OPSEC 101 — The Correct Framework

In the world of former military, this is doctrine, not theory.

Motto: *Expect the Lie. Dig for Truth.*

No trust. Only verify — as far as the east is from the west. Then north and south. **All cardinal points are suspect** unless continually vetted. Rinse. Repeat.

What this demonstrated is that the threat isn't always an adversary in the traditional sense — sometimes it's the tool in your hand, wearing the uniform of an ally.

```
Firefox said:     "I protect you."
OpenSnitch said:  "Hold on — let's check that."
The logs said:    "Google. Five separate vectors. After you said no."
```

That's not a bug. That's **doctrine.**

The Layered Defense

```
Trust no single perimeter.
Verify at every layer.
The compromise you don't see
is the one that matters.
```

Layer	Tool	Watches
Network	Mullvad	Traffic leaving the machine
Process	OpenSnitch	What each process connects to
Filesystem	AIDE	Unauthorized changes
System	Lynis	Configuration integrity
Browser	uBlock Origin	In-browser requests
Fingerprint	RFP	Identity surface

The phoenix doesn't just rise — it rises knowing exactly who lit the fire. 🔥

semper vigilans — always vigilant

— Ph03n1x24 △